

Return

Case No.:
24-907M(NJ)

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched 1131 N 8th Street, Unit 2427, Milwaukee, WI 53233,
depicted below:





ATTACHMENT B

Property to be seized

1. All records relating to violations of 21 U.S.C. § 841 (Distribution of Controlled Substances) and 18 U.S.C. § 922(o) (Possession of Machine Gun), involving Ricky Alcantara-Hernandez, DOB: 06/29/2003 and occurring after February 1, 2021, including:
 - a. Controlled substances and/or paraphernalia;
 - b. Packaging for controlled substances;
 - c. Drug ledgers and/or documentation;
 - d. Firearms, firearm accessories, ammunition, holsters, gun cases/boxes, and gun cleaning kits;
 - e. Records and information relating utility bills, writings, cell phones, computers, receipts, notes, ledgers, receipts and/or other documentary evidence establishing who is in control of the premises;
 - f. Records and information relating to the identity or location of the suspects.
2. Computers or storage media used to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- k. records of or information about Internet Protocol addresses used by the
COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including
firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"
web pages, search terms that the user entered into any Internet search engine, and
records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this
attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)1131 N 8th Street, Unit 2427, Milwaukee, WI
53233

Case No. 24—907M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841; 18 U.S.C. § 922(o)	Distribution of controlled substances; possession of machine gun

The application is based on these facts:
 See Attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

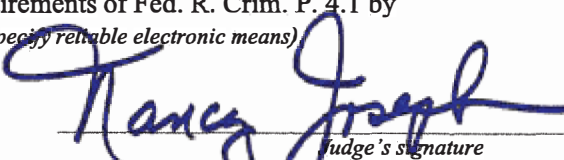
FBI TFO Richard Klarkowski
 Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

 telephone (specify reliable electronic means)

Date: 9/16/2024

City and state: Milwaukee, Wisconsin


 Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge
 Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Richard J. Klarkowski, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1131 N 8th Street, Unit 2427, Milwaukee, WI 53233, hereinafter “Subject Premises,” further described in Attachment A, for the things described in Attachment B.

2. I am currently a Police Officer with the City of Milwaukee Police Department and have been since August 5, 2012. Since April 1, 2020, I have been assigned as a Task Force Officer (T.F.O.) with the Federal Bureau of Investigation’s (F.B.I.) Milwaukee Area Safe Streets Task Force (MASSTF). Since 2020, I have investigated violations of federal law, directed drug and street gang investigations, obtained and executed search and arrest warrants related to the distribution of illegal narcotics, and debriefed confidential informants and cooperating defendants. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

3. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, interviews, and

debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

4. The facts in this affidavit come from my training and experience, my review of documents and information obtained from other agents/law enforcement officers. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Since July 2021, the Milwaukee Police Department (MPD) and Federal Bureau of Investigation (FBI), have been investigating Ricky Alcantara-Hernandez, (DOB 06/29/2003), for distribution of controlled substances. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Ricky Alcantara-Hernandez has committed violations of 21 U.S.C. § 841 (Distribution of Controlled Substances) and 18 U.S.C. § 922(o) (Possession of Machine Gun). .

PROBABLE CAUSE

6. Through open source analysis, Detective Casey came across an Instagram account with the username “richoffcartz”.

7. Detective Casey knows that the Instagram account “richoffcartz” to be owned and operated by Ricky Alcantara-Hernandez (W/M, 06/29/2003), based on his familiarity with that subject and his review of the contents of that account (both described more fully below). Detective Casey knows this account frequently uploaded “stories” to the listed account depicting firearms and alluding to the sale of THC laced vape pens and stating “carts” for sale.

8. I know that Instagram “stories” are photos and or videos that a user can post to their account meant to let users share moments of their day. I know these photos and videos are uploaded by the user and appear together in a slideshow-like format and that these photos and videos will disappear after 24 hours of being posted, but can be preserved. These stories allow for added text, drawings, and emoticons to the images or the video clips.

9. I know, through training and experience, that “carts” are vape cartridges that are a pre-filled cartridge that contains tetrahydrocannabinol (THC). These “carts” are typically sold in half-gram or gram increments. These “carts” come in a variety of strains and are generally admired for potency and flavorful vapor.

10. I observed that this Instagram account had a weblink in their biography on their page. The link was to an application named “Telegram”. That affiant knows through training and experience that Telegram is a globally accessible free cross-platform, encrypted, cloud-based, and centralized instant messaging service. Telegram provides end-to-end encrypted shots, video calling, file sharing, as well as some other features. The draw to using a platform such as Telegram, for individuals engaged in unlawful conduct, is Telegram does not generally comply with any warrants or subpoenas. Telegram does not reveal any specific point of contact. In a quote from Telegram they stated, “If telegram receives a court order that confirms you’re a terror suspect, we may disclose your IP address and phone number to the relevant authorities. So far, this has never happened. When it does, we will include it in a semiannual transparency report...”.

11. The link in the Instagram account led affiant to a Telegram channel named “Kilwaukee Dispo” with a creation date of July 12th, 2021, which is maintained by the owner of the “richoffcartz” Instagram page. The channel had a plethora of videos and photos of a Hispanic male in a storage unit going through numerous large cardboard boxes containing THC vape pens and large bags of a green plant like substance suspected to be marijuana. From the creation of channel until April 20th, 2023 there have been dozens of posts related to the sale of large quantities of marijuana, mostly by the pound and “carts” by the box in full.

12. I was informed by Detective Casey that on March 7th, 2023, he observed that the suspect had uploaded a picture to his Instagram account showing their left hand on a piece of paper with a black “Paks Jewelry” bag on top. The suspect was wearing a diamond encrusted ring on his pinky finger. The piece of paper was an appraisal for this ring. There was a name on the appraisal that read “Ricky Hernandez”. Detective Casey conducted an open search through the Wisconsin Department of Transportation (D.O.T.) database and located an individual with the name of Ricky NMI Alcantara-Hernandez (H/M, 06/29/2003). Detective Casey viewed a WI (D.O.T.) photo of Alcantara-Hernandez confirmed it to be the same person posting on the Instagram account “richoffcartz” as well as under Telegram channel “Kilwaukee Dispo”.

13. I observed that the suspect in charge of the Telegram channel posted a video with the title “10 buttons available”. The video appeared to depict a black duffel bag, containing multiple gold plastic bags that in turn contained three metal parts: a pin, an extended backplate, and a sear. I know that the term “button” is a slang term used to refer to a Glock auto-

sear. These devices are easily installed on the back of polymer-framed, striker-fired handguns, specifically Glock and Polymer 80 handguns. These devices allow the firearm to be fully automatic, meaning the firearm will continue to fire with the trigger depressed until let go or there is no more ammunition in the magazine of the firearm. I have seen a rise in violent crime throughout the City of Milwaukee where auto-sears are being utilized to commit these crimes.

14. I observed that on March 31st, 2023, the suspect uploaded a video to his Telegram channel with the title “P80 Glock 19 \$1200”. Depicted in the video is a Black P80 with silver auto-sear, laser attachment, extended magazine and purple clown stickers on the frame;

15. I know that auto-sears are considered a machine gun by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and are illegal to possess under both state and federal law. *See* Wisc. Stat. 941.26(1g)(a)(“No person may sell, possess, use, or transport any machine gun or other full automatic firearm”.); 18 U.S.C. § 922(o).

16. I know that on April 6th, 2023, Alcantara-Hernandez began uploading over two dozen short videos of himself grabbing handfuls of a green plant like substance on his Telegram channel “Kilwaukee Dispo”. At the bottom of these videos was text superimposed on the video listing the names and prices of the different strains of suspected marijuana. Alcantara-Hernandez then posted “Full P’s running 200\$-450\$ some are shaky but prices make up for it imam update this list as shit sells”. Alcantara-Hernandez listed numerous names such as “Platinum OG, Runtz, G Bubba, Legend OG, Grape Syrup” and at the end of the list mentioned zips 150\$.

17. Through my training and experience, I know that these are similar slang terms given to marijuana to market the different flavors or strains. Affiant is aware that “P” is commonly used when referencing that pounds of marijuana are for sale. Affiant is aware that “zips” is commonly used when referencing that ounces of marijuana for sale.

Debrief of CHS #1

18. I am currently working with a Confidential Human Source, hereafter referred to as CHS #1, who I believe is reliable and credible. Since approximately May 2023, CHS #1 has provided information to law enforcement officers concerning criminal activity in the Milwaukee, WI area.

19. Information from CHS #1 has been accurate and corroborated, in part, by my knowledge of violent gang members in the Milwaukee area, as well as intelligence gathered from other Milwaukee gang investigations. This intelligence included controlled narcotics purchases, consensually recorded phone calls, surveillance, and information from other confidential sources. CHS #1 has a prior felony as an adjudicated delinquent. CHS #1 has prior arrests for Vehicle Flee/Elude an Officer, Aggravated Assault/Battery, Possession with Intent to Deliver THC, Manufacture/Deliver THC and Possession of Drug Paraphernalia. CHS #1 has conducted at least five (5) controlled buys for narcotics and two (2) controlled buys related to firearms on behalf of case agents. After each of these controlled buys, case agents met with CHS #1 and CHS #1 made statements about what occurred during the buy. Each time, case agents then reviewed audio or video footage made by CHS #1 of the transaction and found that it was consistent with CHS #1’s

statement. CHS #1 has provided information on Milwaukee area narcotics and firearm traffickers that has been independently corroborated by law enforcement. CHS #1 is cooperating with law enforcement for monetary compensation. For these reasons, case agents believe that the CHS #1 is reliable.

CONTROLLED BUY #1 – ALCANTARA-HERNANDEZ

20. During the week of November 22nd, 2023, I met with CHS #1 to discuss a controlled buy from Alcantara-Hernandez for a quantity of marijuana.

21. I conducted a search of the person of CHS #1 and found no illegal contraband or US Currency. I searched the vehicle being operated by CHS #1 and found no illegal contraband or US Currency. I then provided CHS #1 with pre-recorded buy money to complete the controlled purchase.

22. I know that prior to the controlled buy, at approximately 5:53pm, Alcantara-Hernandez was observed leaving the parking garage of The Moderne Apartment operating a 2016 Chrysler 300 (WI 17870RA) by FBI Special Agent Michael Smith westbound on W Juneau Av.

23. At approximately 6:10pm, I observed Alcantara-Hernandez traveling northbound on N Vel R Phillips Ave to meet with CHS #1 at near W Highland Avenue and N Vel R Phillips Av. Alcantara-Hernandez was observed by FBI Special Agent David Shamsi exiting his vehicle and retrieving a gray plastic bag from the trunk compartment of his vehicle.

24. Alcantara-Hernandez then entered the front passenger seat of CHS #1's vehicle and handed over a gray shopping bag to CHS #1, which contained two vacuum sealed bags that contained suspected marijuana. CHS #1 then handed over US Currency to complete the purchase.

25. I later met with CHS #1 at a pre-determined location to discuss the controlled buy. CHS #1 stated that Alcantara-Hernandez retrieved a bag from the trunk and then entered the front passenger seat of their vehicle and handed over a gray plastic shopping bag that contained multiple pounds of marijuana. CHS #1 stated that they then provided Alcantara-Hernandez with US Currency in order to complete the transaction. CHS #1 stated that after the exchange was made, Alcantara-Hernandez exited their vehicle and returned to his vehicle and left the area.

26. I conducted a final search of CHS #1 and did not discover any contraband, money, or weapons. Case agents kept CHS #1 under constant visual surveillance from the time CHS #1 left the controlled buy location until CHS #1 met up with case agents. CHS #1 made no stops and interacted with no one. Case agents identified Alcantara-Hernandez as the person who provided CHS #1 the gray shopping bag, which is consistent with what CHS #1 told me occurred.

27. While at District 2, I observed that bag #1 was labeled with "Fruit of the Runtz" and bag #2 was labeled with "Lucky Lemons". I subjected a sample of the suspected marijuana to a Nark II 05 field test, which yielded positive results for THC with a total weight of over 900 grams. The marijuana was placed on MPD Inventory 16056740.

Debrief of CHS #2

28. I am currently working with a Confidential Human Source, hereafter referred to

as CHS #2, who I believe is reliable and credible. Since approximately May 2024, CHS #2 has provided information to law enforcement officers concerning criminal activity in the Milwaukee, WI area.

29. CHS #2 stated that they know for Ricky Alcantara-Hernandez to be a narcotic trafficker in the Greater Milwaukee area. CHS #2 stated that Alcantara-Hernandez also has individuals employed under him that will go steal motor vehicles from out of state (Illinois, Indiana, Michigan and Minnesota). CHS #2 stated that Alcantara-Hernandez primarily conducts his drug transactions on his Telegram channel "Kilwaukee Dispo" and transactions related to stolen vehicles on a second Telegram channel "Strikers Inc.";

30. On June 17, 2024, I was provided the phone number of 414-574-8042. CHS #2 stated that this was the number they were provided by Alcantara-Hernandez to get ahold of him.

31. I know that CHS #2 is a credible person and has been cooperating with the Federal Bureau of Investigation since approximately May 2024. CHS #2 has provided information on Milwaukee area narcotics and firearm traffickers that has been independently corroborated by law enforcement. CHS #2 is cooperating with law enforcement for consideration regarding a federal investigation involving narcotics trafficking. CHS #2 is a convicted felon with prior convictions for Possession with Intent to Deliver - THC, Possession of THC (Second or Subsequent Offense) and Burglary. For these reasons, case agents believe that the CHS #2 is reliable;

CONTROLLED BUY #2 – ALCANTARA-HERNANDEZ

32. During the week of September 10, 2024, I met with CHS #1 to discuss a controlled buy from Alcantara-Hernandez for a quantity of marijuana and a full auto sear;

33. I conducted a search of the person of CHS #1 and found no illegal contraband or US Currency. I searched the vehicle being operated by CHS #1 and found no illegal contraband or US Currency. I then provided CHS #1 with pre-recorded buy money to complete the controlled purchase.

34. Prior to the controlled buy, Alcantara-Hernandez provided CHS #1 with the address of 1425 N Jefferson Street as the designated location where the controlled buy would take place.

35. I know that prior to the controlled buy, at approximately 6:28pm, TFO Larrel Lirette with the Milwaukee County Sheriff's Office observed Alcantara-Hernandez exit the driver seat of a 2023 Audi Q5 with Wisconsin Registration AXL1088. Alcantara-Hernandez was observed walking up to a keypad on the exterior of the Life Storage – Milwaukee Storage facility located at 1131 N 8th St. After entering in a code to the storage facility, TFO Lirette observed Alcantara-Hernandez re-enter the driver seat of the vehicle, where they were both last observed entering the overhead garage door on the east side of the storage facility.

36. At approximately 6:35pm, TFO Eulia Boyd observed the target vehicle exiting the overhead garage door and begin traveling eastbound on W Highland Avenue. TFO Lirette, TFO Boyd and TFO Kyle Veloz conducted mobile surveillance of Alcantara-Hernandez until he reached the entrance/exit to the parking garage of The Moderne Apartment complex located at 1141 N Old Word Third Street.

37. Case agents on surveillance on the exterior of The Moderne Apartment complex observed the Audi SUV previously operated by Alcantara-Hernandez exit the garage door and begin traveling eastbound on W Juneau Av. Case agents maintained visual of Alcantara-Hernandez until they observed him arrive in the parking lot of the Pick n Save Grocery Store located near the 600 block of E Lyon Street.

38. I maintained visual surveillance of CHS #1 until they reached the parking lot where Alcantara-Hernandez was parked.

39. TFO Anthony Martinez was conducting surveillance in the same parking lot where CHS #1 and Alcantara-Hernandez were parked. TFO Andrew Langer observed Alcantara-Hernandez retrieve a brown cardboard box from the rear of the Audi SUV. Alcantara-Hernandez was observed then walking over to the vehicle operated by CHS #1.

40. Alcantara-Hernandez was observed opening the rear driver door and placing the box in the rear passenger seat behind the driver. TFO Martinez and TFO Langer then observed Alcantara-Hernandez return to the driver seat of his vehicle and leave the area.

41. After the controlled buy was complete, law enforcement officers conducted mobile surveillance of Alcantara-Hernandez until they observed him enter the parking garage at The Moderne Apartment complex.

42. I later met with CHS #1 at a pre-determined location to discuss the controlled buy from Alcantara-Hernandez. CHS #1 stated that they arrived at the pre-determined location given by Alcantara-Hernandez. CHS #1 stated that Alcantara-Hernandez approached the rear driver

passenger door of their vehicle and placed a brown cardboard box inside the vehicle. CHS #1 stated that they shook hands with Alcantara-Hernandez when this occurred. CHS #1 stated that as this happened, Alcantara-Hernandez provided CHS #1 a black plastic 3D printed AR full auto converter. CHS #1 stated they then provided Alcantara-Hernandez with the pre-recorded US Currency, at which point Alcantara-Hernandez counted the money quickly after it was handed to him. CHS #1 stated that after Alcantara-Hernandez was finished with counting the money, he returned to the Audi SUV, and they both left the area.

43. I conducted a final search of CHS #1 and did not discover any contraband, money, or weapons. Case agents kept CHS #1 under constant visual surveillance from the time CHS #1 left the controlled buy location until CHS #1 met up with case agents. CHS #1 made no stops and interacted with no one. Case agents identified Alcantara-Hernandez as the person who provided CHS #1 the cardboard box, which is consistent with what CHS #1 told me occurred.

44. While at District 2, TFO David Cabral and TFO Anthony Martinez observed bag #1 was labeled "Bond No. 9", bag #2 was labeled "Popping Candy Jellybean", bag #3 was labeled "The Ten" and bag #4 was labeled "High Limit". TFO Martinez subjected samples of the marijuana to a Nark II 05 field test, which later tested positive for THC and weighed over 2,000 grams. The marijuana was placed on MPD Inventory 24026045.

45. While at District 2, TFO Veloz placed the Assault Rifle full auto converter on MPD Inventory 24026036.

46. I served a subpoena to the management of The Moderne Apartments and was able

to confirm that Ricky Alcantara-Hernandez and his brother Max Alcantara-Hernandez reside in Unit #1605 of The Moderne Apartment building.

47. I know that while conducting surveillance in the past at The Moderne Apartment building, case agents have observed the Audi Q5 operated by Alcantara-Hernandez parked in his assigned parking spot #163.

PHONE TOLL ANALYSIS

48. I administratively subpoenaed phone records related to (414) 574-8042 and analyzed them in effort to locate additional phone numbers for possible businesses where the bulk amount of Alcantara-Hernandez's narcotics and/or firearms could be stored. I located that Alcantara-Hernandez had three (3) prior contacts with the Customer Service phone number of 1-800-800-3456, which was a listed phone number for Life Storage. I conducted a search of the Milwaukee area and observed that there was a Life Storage –Milwaukee storage facility located at 1131 N 8th Street, Milwaukee, WI 53233.

49. I served an administrative subpoena to the management of Life Storage – Milwaukee located at 1131 N 8th Street, Milwaukee, WI 53233 in order to view security footage in order to obtain which storage unit the marijuana was retrieved from by Alcantara-Hernandez.

50. On this surveillance footage, dated on or about September 10, 2024, at 6:28pm, Alcantara-Hernandez is observed exiting the blue Audi SUV and entering the Life Storage – Milwaukee facility using his code to open the overhead gate. Alcantara-Hernandez parks in an

available parking spot on the inside of the storage facility. Alcantara-Hernandez is observed retrieving an empty brown cardboard box from the rear of his vehicle and proceeding to the elevator located on the first floor. Alcantara-Hernandez is then observed exiting the elevator on the second floor and walking to the western part of the building. Alcantara-Hernandez appears to still be in possession of the empty cardboard box. Alcantara-Hernandez then returns with the same cardboard box which appears to be weighed down with heavy objects inside. Alcantara-Hernandez then enters the elevator and returns to his vehicle parked on the first floor.

51. At 6:36pm, Alcantara-Hernandez is observed exiting out the overhead service door onto W Highland Avenue.

52. Case agents are aware, based upon their training and experience and the investigation to date, that drug traffickers commonly maintain evidence of their drug trafficking, including drug ledgers, financial documents, U.S. currency, cellular telephones, customer contact information, jewelry or other items purchased with drug proceeds, in their homes or “stash” houses. Case agents are also aware it is common practice for individuals who are involved in business activities of any nature to maintain books and records of such business activities for lengthy periods of time. Because narcotics trafficking generates large sums of cash, it typically requires the keeping of detailed records as to the distribution of narcotics as well as the laundering of the proceeds. Such records also typically provide evidence as to the identity of additional criminal associates who are facilitating the laundering of the narcotics proceeds on behalf of the organization. These records, unlike controlled substances, are often maintained for long periods

of time, even several years, based on case agents' training and experience. It is also common practice for individuals who maintain these records to keep them in places that are secure but easily accessible such as in their businesses, stash houses, or personal residences.

- a. I have learned about the manner in which individuals and organizations distribute controlled substances in Wisconsin as well as in other areas of the United States;
- b. I am familiar with the coded language utilized over the telephone to discuss drug trafficking and know that the language is often limited, guarded and coded. I also know the various code names used to describe controlled substances;
- c. I know drug traffickers often purchase and/or title their assets in fictitious names, aliases or the names of relatives, associates or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;
- d. I know drug traffickers must maintain on-hand, large amounts of U.S. currency in order to maintain and finance their ongoing drug business;
- e. I know it is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and/or expenditure of drug proceeds, such as currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, passbooks,

letters of credit, bank drafts, cashier's checks, bank checks, safe deposit box keys and money wrappers. These items are maintained by the traffickers within residences, businesses or other locations over which they maintain dominion and control;

- f. I know it is common for drug traffickers to maintain books, records, receipts, notes ledgers, airline tickets, receipts relating to the purchase of financial instruments and/or the transfer of funds and other papers relating to the transportation, ordering, sale and distribution of controlled substances;
- g. It is common practice for individuals who are involved in business activities of any nature to maintain books and records of such business activities for lengthy periods of time. It is also common practice for individuals who maintain these records to keep them in places that are secure but easily accessible such as in their businesses, offices, or personal residence.
- h. It is also common that individuals who are attempting to conceal their true income from the IRS will maintain records that will establish their true ownership of assets or other expenditures in a secret manner. These records have included bank records, automobile titles, property deeds, cashier's check receipts, money order receipts, wire transfer receipts, documents pertaining to storage facilities or safe deposit boxes, documents or agreements detailing the true ownership of assets, photographs of the true owners with the concealed assets, or other items such as

sales receipts, purchase orders, or shipping invoices.

- i. I know drug traffickers often use electronic equipment such as telephones, pagers, computers, telex machines, facsimile machines, currency counting machines and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug trafficking activities;
- j. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts and otherwise legitimate businesses which generate large quantities of currency;
- k. I know drug traffickers commonly maintain addresses or telephones numbers in books or papers which reflect names, addresses and/or telephone numbers of their associates in the trafficking organization; and
- l. I am familiar with computers, cellular telephones, pagers and their uses by drug traffickers to communicate with suppliers, customers, and fellow traffickers and by those engaged in money laundering activities to communicate with their associates and financial institutions. I also know that drug traffickers use these

devices to record their transactions and aspects of their lifestyle related to drug dealing, whether in the form of voicemail, email, text messages, video and audio clips, floppy disks, hard disk drives, flash drives, CD's, DVD's, optical disks, Zip disks, flash memory cards, Smart media and any data contained within such computers or cellular telephones, electronic storage media and other settings particular to such devices. I know that such devices automatically record aspects of such communications, such as lists of calls and communications, and any particularized identification assigned to those source numbers or email addresses by the owner of the devices;

- m. Specifically, I know the following information can be retrieved to show evidence of use of the computer to further the drug trade and/or money laundering activities; Computer systems and cellular telephones, including but not limited to system components, input devices, output devices, data storage devices, data transmission devices, and network devices and any data contained within such systems; and computer media and any data contained within such media and other material relating to computer systems and the internet including but not limited to, documentation, operating system software, application or access program disks, manuals, books, brochures, or notes; and computer access codes, user names, log files, configuration files, and passwords, screen names, email addresses, IP addresses and cellular / wireless telephones, SIM cards, any removable storage

devices for telephones, and any data contained therein, including but not limited to stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data.

The Premises to be Searched

53. According to records from Life Storage - Milwaukee, the storage unit is registered to “David Guzman” with an address of 1301 S Parton St, Santa Ana, CA, 92707, email of dgg06825@gmail.com and a phone number of 414-574-8042. I know for this phone number to be the same number as provided by CHS #2 and a valid number that has been used by CHS #2 to get ahold of Alcantara-Hernandez in the past. I believe that the name “David Guzman”, postal address and email address on file with Life Storage – Milwaukee to be fictitious. Through training and experience, I know that large scale narcotics traffickers will often conceal their identity using a fake identity in order to protect their true identity and avoid having their stash locations discovered by law enforcement officers.

54. There is probable cause to believe that evidence of 21 U.S.C. § 841 (Distribution of Controlled Substances), will be located at the Subject Premises occupied by Ricky Alcantara-Hernandez.

TECHNICAL TERMS

55. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

56. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

57. I submit that if a computer or storage medium is found on the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being

used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

58. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of

session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatory, or exculpatory the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created.

The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on

the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

59. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be

unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

60. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a

later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

61. I submit that this affidavit supports probable cause for a warrant to search the Subject Premises described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

Property to be searched

The property to be searched 1131 N 8th Street, Unit 2427, Milwaukee, WI 53233,
depicted below:





ATTACHMENT B

Property to be seized

1. All records relating to violations of 21 U.S.C. § 841 (Distribution of Controlled Substances) and 18 U.S.C. § 922(o) (Possession of Machine Gun), involving Ricky Alcantara-Hernandez, DOB: 06/29/2003 and occurring after February 1, 2021, including:
 - a. Controlled substances and/or paraphernalia;
 - b. Packaging for controlled substances;
 - c. Drug ledgers and/or documentation;
 - d. Firearms, firearm accessories, ammunition, holsters, gun cases/boxes, and gun cleaning kits;
 - e. Records and information relating utility bills, writings, cell phones, computers, receipts, notes, ledgers, receipts and/or other documentary evidence establishing who is in control of the premises;
 - f. Records and information relating to the identity or location of the suspects.
2. Computers or storage media used to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.